(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－8851

(43)公開日　平成８年(1996)１月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｈ	1/00		Ｆ			
Ｈ０４Ｌ	9/00					
	9/10					
	9/12					
				Ｈ０４Ｌ	9/00	Ｚ

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平6－134667

(22)出願日　平成６年(1994)６月16日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　神竹　孝至
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　前田　賢一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

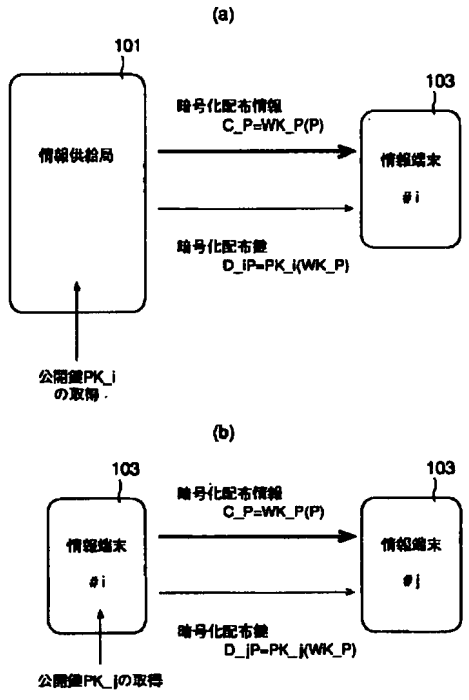
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　情報配布システムおよび情報配布方法

(57)【要約】

【目的】　有料情報の１次・２次配布ができ、端末の物理的安全性が保証されなくなっても被害がその端末装置以外に及ばない情報配布システムを得ること。

【構成】　供給局から複数の端末に及び端末間で情報伝達媒体を介しデジタル情報を配布する情報配布システムにおいて、供給局は、該情報毎に固有の第１暗号鍵で該情報を暗号化した暗号化情報と、受信端末固有の第２暗号鍵で第１暗号鍵に対応する第１復号鍵を暗号化した配布鍵を該媒体に出力する手段を備え、端末夫々は、供給局又は他端末から該媒体を介し伝達された暗号化情報と配布鍵を入力する手段と、第２暗号鍵に対応する第２復号鍵で配布鍵を復号し取出した第１復号鍵で暗号化情報を復号する手段と、暗号化配布鍵を第２復号鍵で復号し取出した第１復号鍵を暗号化情報の伝達先の端末固有の第２暗号鍵で暗号化する手段と、この手段で得た配布鍵と暗号化情報を該媒体に出力する手段を備える。



【特許請求の範囲】
【請求項１】ディジタル情報の配布を行う情報供給局と、前記ディジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記ディジタル情報を２次的に配布する情報配布システムにおいて、
前記情報供給局は、
前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を伝達すべき前記情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵とを前記情報伝達媒体に出力する手段を備え、
前記情報端末夫々は、
前記情報供給局または他の前記情報端末から前記情報伝達媒体を介して伝達された前記暗号化ディジタル情報および前記暗号化配布鍵を入力する入力手段と、
前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第１の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、
前記暗号化配布鍵を前記第２の復号鍵を用いて復号した後、この復号により得られる前記第１の復号鍵を、前記暗号化ディジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第２の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、
この暗号化配布鍵変換手段により得られる前記暗号化配布鍵と前記暗号化ディジタル情報とを前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする情報配布システム。
【請求項２】前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、
前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、
前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記ディジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする請求項１に記載の情報配布システム。
【請求項３】前記復号手段および前記暗号化配布鍵変換手段は、外部から物理的に保護された領域に設けられたことを特徴とする請求項１に記載の情報配布システム。
【請求項４】ディジタル情報の配布を行う情報供給局と、前記ディジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記ディジタル情報を２次的に配布する情報配布システムにおいて、
前記情報供給局は、
前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報およびこの暗号化ディジタル情報を伝達すべき前記情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵、または該暗号化配布鍵のみを前記情報伝達媒体に出力する手段を備え、
前記情報端末夫々は、
前記情報伝達媒体を介して、前記情報供給局から伝達された前記暗号化ディジタル情報および前記暗号化配布鍵または、他の前記情報端末から伝達された前記暗号化ディジタル情報および前記情報供給局から伝達された前記暗号化配布鍵を入力する入力手段と、
前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第１の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、
前記暗号化ディジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする情報配布システム。
【請求項５】前記情報供給局は、前記情報端末夫々に対する前記暗号化配布鍵の配布行為を記録する手段をさらに備え、
前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、
前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、
前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記ディジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする請求項４に記載の情報配布システム。
【請求項６】前記復号手段は、外部から物理的に保護された領域に設けられた特徴とする請求項４に記載の情報配布システム。
【請求項７】第１の情報端末が、ディジタル情報の配布を受けるとともに、受けたディジタル情報を第２の情報端末に２次的に配布する情報配布方法において、
前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジ

タル情報と、前記第１の情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵とを入力する入力ステップと、
前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号する復号ステップと、
この復号ステップにより得られる前記第１の復号鍵を、前記第２の情報端末に固有に割り当てられた前記第２の暗号鍵を用いて暗号化する暗号化ステップと、
この暗号化ステップにて得られる前記暗号化配布鍵と前記暗号化ディジタル情報とを出力する出力ステップとを有することを特徴とする情報配布方法。
【請求項８】第１の情報端末が、ディジタル情報の配布を受けるとともに、受けたディジタル情報を第２の情報端末に２次的に配布する情報配布方法において、
前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報および前記第１の情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵を入力する入力ステップと、
前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号する処理および前記暗号化ディジタル情報を出力する処理の少なくとも一方を行うステップとを有することを特徴とする情報配布方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、ディジタル化された著作物の流通において、著作者の権利を保証しつつ、利用者はその閲覧および編集が可能となる情報配布システムおよび情報配布方法に関する。
【０００２】
【従来の技術】近年のディジタル通信や計算機技術等の発展により、画像・音声・テキストなどの様々な情報をディジタル化し統合的に取り扱うことが可能となりつつある。このような技術は各適用分野で導入が検討されており、例えば情報配布に関する分野では、ディジタル化された新聞、雑誌、音楽、映画、…などの著作物を情報利用者がネットワークを介して受信できるシステムがいくつか提案されている。
【０００３】しかしながら、この種の情報配布システムを実際に構築しようとすると、著作権保護という重要な問題が顕在化してくる。すなわち、上記システムで扱うディジタル情報にはアナログ情報にない特徴として、完全な複製を容易に、しかも無尽蔵に作成できる優れた点がある。これは利用者にとっては大きな利点であるが、著作物を提供する側にとっては権利保護の面で問題である。従って、上記システムを完全なものにするためには、ディジタル情報の特徴を損なわずにしかも著作権を保護できるような仕組みが必須となるのである。
【０００４】このような問題は、有償なディジタル情報のさきがけともいえるソフトウェア（プログラム）の配布において既に発生している。そして、著作権保護を法律による規制に委ねるのみでは自ずと限界があるため、技術的な対策が検討されている。以下、ソフトウェアの配布において著作権保護のために講じられている２つの対策を説明する。
【０００５】１つめの方法は、特定の計算機でしか実行できない形式にソフトウェアを変換して配布する方法である。すなわち、計算機に固有のＩＤを割り当てるとともに、ソフトウェアの販売時に利用者の計算機ＩＤを販売ソフトに織り込んでおく。ソフトウェアの実行時には、計算機ＩＤとソフトウェア内のＩＤとを比較し、一致しなければ起動されないようにする。ただし、ソフトウェアの一部に計算機ＩＤコードを書き込むだけでは、その書き込み位置さえ判れば簡単にプロテクトが破られてしまう。そこで、拡張法として暗号技術を利用し、ソフトウェア全体をある鍵で暗号化しておき、その鍵を個別の計算機ごとにカスタマイズして配布する方法が提案されている。具体的には、次の通りである。計算機には固有の鍵（ここでは端末鍵と呼ぶ）が格納されており、その鍵と復号器は利用者からも保護されている。ソフト提供者は、ソフトウェアを固有の鍵（ここではソフト鍵と呼ぶ）で暗号化するとともに、用いたソフト鍵を端末鍵で暗号化した鍵データを作成する。販売時には、ユーザーに暗号化されたソフトウェアおよび鍵データを組にして提供する。鍵データはソフト鍵を端末鍵で暗号化したものであるので、特定の計算機おいてのみ鍵データを復号してソフト鍵を取得することができる。そして、このソフト鍵を用いて暗号化されたソフトウェアを復号し実行できる。
【０００６】２つめの方法は、ソフトウェアの利用に対して課金を行ない、ソフトウェアの配布は無料とするものである。従来からある課金に対する考え方の基本は（流通＝課金対象）でありソフトウェアの取得行為に対して課金する方法とみなすことができるが、この方法においては流通は無料にする代りに（利用＝課金対象）とする方がディジタル情報提供サービスには適するという考えに基づくものである。この方法の具体例としては、“超流通”と呼ばれる方式がある。なお、超流通は、次の文献に詳しい。
・森亮一，田代秀一：“ソフトウェア・サービス・システム（ＳＳＳ）の提案”，電子情報通信学会論文誌，Ｖｏｌ．Ｊ７０Ｄ，Ｎｏ．１，ｐｐ．７０－８１．・Ｒｙｏｉｃｈｉ Ｍｏｒｉ，Ｍａｓａｊｉ Ｋａｗａｈａｒａ：“Ｓｕｐｅｒｄｉｓｔｒｉｂｕｔｉｏｎ：Ｔｈｅ Ｃｏｎｃｅｐｔ ａｎｄ ｔｈｅ Ａｒｃｈｉｔｅｃｔｕｒｅ”，Ｔｒａｎｓ．ｏｆ ＩＥＩＣＥ，Ｖｏｌ．Ｅ７３，Ｎｏ．７，ｐｐ．１１３３－１１４６．

超流通の基本コンセプトは、以下の通りである。
（１）情報利用者は、ディジタル情報をほとんど無料で入手できる。すなわち、販売店から購入する以外に、人からコピーをもらう形態も許す。
（２）情報利用者の端末には、課金管理を行う装置が内蔵されており、情報を実際に利用するごとに課金装置に記録されていく。すなわち、使用量に応じて課金される。
（３）情報利用者はプリペイド方式あるいはクレジット方式などにより情報の利用可能度数を表すデータ（共通クレジットと呼ばれる）を購入し、その共通クレジットを端末に渡すことによりディジタル情報を利用できる。
【０００７】このように利用行為に対して課金できる仕組みを構築することにより、著作権保護を実現するだけでなく、コピーしても元の情報からの劣化が生じないディジタル情報の特徴を積極的に利用することにより流通コストを極端に下げ、実質的なソフト単価を著しく低く抑えることを可能にするのが超流通のねらいである。
【０００８】超流通においては、ソフトウェアを利用するごとに課金できるような仕組みをどのように実現するかが最も重要となる。具体例としては、配布されるソフトウェアは、ソフトウェア本体とその実行処理に対する課金管理を行うプログラムの２つで構成されており、いずれも暗号化された状態で流通される。ユーザ計算機には課金管理を行うモジュールが存在し、そのモジュールは暗号ソフトの復号を行い、ソフトウェアに添付された課金プログラムを起動する。課金プログラムは配布ソフトの使用状況を監視し、被課金行為が発生するごとに共通クレジットの減額を行う。共通クレジットがある値以上でないとソフトウェアは起動できないようにする。ソフトウェアを再起動するためには、サービスセンタに通信回線によりアクセスし、ある額のクレジット情報を購入する。この課金管理のモジュールは、ユーザの不正使用から保護されていなければならない。また、超流通では、コピーそのものを渡すだけで同一の暗号化ソフトがどの端末でも動作することを想定しているため、どの課金モジュールにも共通の暗号鍵が記憶されるものとしている。
【０００９】以上のように、従来からソフトウェアに対する著作権保護を可能とする技術が検討されている。しかしながら、このようなソフトウェアに対して考案された著作権保護技術は、そのまま他のディジタル情報に転用することを考えた場合、十分でない面がある。例えば、新聞における記事の切抜きやビデオ映像におけるダビング編集など、いわゆるディジタル情報の２次使用に関する著作権保護や課金の問題である。すなわち、上記超流通は、ディジタル情報の２次使用を考慮していないので、２次使用が日常的に行われるであろう現実の情報配布システムに適用することは極めて困難である。もちろん、２次使用を禁止すれば、著作権者の利益は守られるが、その一方で利用者の自由を大きく制限することになってしまう。
【００１０】また、超流通のように情報の利用と課金を一体化するシステムでは、万一、保護装置が破られた場合に、システム全体に被害が波及するおそれがあるが、この点は保証されていない。
【００１１】
【発明が解決しようとする課題】以上説明したように、従来の情報配布システムでは、情報の２次使用に対する著作権保護や課金の技術が十分でなかった。また、情報の利用と課金を一体化するシステムでは、万一、復号鍵等を格納している保護装置が破られた場合にシステム全体に被害が波及するおそれがあった。
【００１２】本発明は、上記事情に鑑みてなされたものであり、有料のディジタル情報の配布は供給局から行なうだけでなく、既にそのディジタル情報を取得している端末間での２次配布も可能であり、万一端末装置の物理的安全性が保証されなくなったとしても被害がその端末装置以外に及ばない情報配布システムおよび情報配布方法を提供することを目的とする。また、ディジタル情報の配布自体は無償とし、ディジタル情報の利用時に課金することのできる情報配布システムおよび情報配布方法を提供することを目的とする。
【００１３】
【課題を解決するための手段】上記目的を達成するために本発明（請求項１）では、ディジタル情報の配布を行う情報供給局と、前記ディジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記ディジタル情報を２次的に配布する情報配布システムにおいて、前記情報供給局は、前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を伝達すべき前記情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵とを前記情報伝達媒体に出力する手段を備え、前記情報端末夫々は、前記情報供給局または他の前記情報端末から前記情報伝達媒体を介して伝達された前記暗号化ディジタル情報および前記暗号化配布鍵を入力する入力手段と、前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第１の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、前記暗号化配布鍵を前記第２の復号鍵を用いて復号した後、この復号により得られる前記第１の復号鍵を、前記暗号化ディジタル情報を伝達すべき別の前記情報端末に固有に割り当てられた前記第２の暗号鍵を用いて暗号化する暗号化配布鍵変換手段と、この暗号化配布鍵変換手段により得られる前記暗号化配布

鍵と前記暗号化ディジタル情報とを前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする。

【００１４】好ましくは、前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記ディジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする。

【００１５】また、好ましくは、前記復号手段および前記暗号化配布鍵変換手段は、外部から物理的に保護された領域に設けられたことを特徴とする。また、本発明（請求項４）では、ディジタル情報の配布を行う情報供給局と、前記ディジタル情報を受ける複数の情報端末と、前記情報供給局および前記複数の情報端末の相互間を接続する情報伝達媒体とから構成されるとともに、各情報端末間では前記情報供給局から配布された前記ディジタル情報を２次的に配布する情報配布システムにおいて、前記情報供給局は、前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報およびこの暗号化ディジタル情報を伝達すべき前記情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵、または該暗号化配布鍵のみを前記情報伝達媒体に出力する手段を備え、前記情報端末夫々は、前記情報伝達媒体を介して、前記情報供給局から伝達された前記暗号化ディジタル情報および前記暗号化配布鍵または、他の前記情報端末から伝達された前記暗号化ディジタル情報および前記情報供給局から伝達された前記暗号化配布鍵を入力する入力手段と、前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号した後、この復号により得られる前記第１の復号鍵を用いて前記暗号化ディジタル情報を復号する復号手段と、前記暗号化ディジタル情報を前記情報伝達媒体に出力する出力手段とを備えたことを特徴とする。

【００１６】好ましくは、前記情報供給局は、前記情報端末夫々に対する前記暗号化配布鍵の配布行為を記録する手段をさらに備え、前記情報端末夫々は、前記復号手段により得られる前記暗号化ディジタル情報を編集するための編集手段と、前記暗号化ディジタル情報または前記復号手段により復号されたディジタル情報を利用するごとに更新される利用可能度数情報を格納する利用可能度数情報格納手段と、前記復号手段による前記暗号化ディジタル情報の復号行為および前記編集手段による前記ディジタル情報の編集行為に応じた利用情報の記録を生成するとともに、前記復号行為および前記編集行為に応じて前記利用可能度数情報格納手段に格納された前記利用可能度数情報の更新を行う利用管理手段とをさらに備えることを特徴とする。

【００１７】また、好ましくは、前記復号手段は、外部から物理的に保護された領域に設けられた特徴とする。一方、本発明（請求項７）では、第１の情報端末が、ディジタル情報の配布を受けるとともに、受けたディジタル情報を第２の情報端末に２次的に配布する情報配布方法において、前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報と、前記第１の情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵とを入力する入力ステップと、前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号する復号ステップと、この復号ステップにより得られる前記第１の復号鍵を、前記第２の情報端末に固有に割り当てられた前記第２の暗号鍵を用いて暗号化する暗号化ステップと、この暗号化ステップにて得られる前記暗号化配布鍵と前記暗号化ディジタル情報とを出力する出力ステップとを有することを特徴とする。

【００１８】また、本発明（請求項８）では、第１の情報端末が、ディジタル情報の配布を受けるとともに、受けたディジタル情報を第２の情報端末に２次的に配布する情報配布方法において、前記ディジタル情報ごとに固有に割り当てた第１の暗号鍵を用いて該ディジタル情報を暗号化した暗号化ディジタル情報および前記第１の情報端末に固有に割り当てられた第２の暗号鍵を用いて該第１の暗号鍵に対応する第１の復号鍵を暗号化した暗号化配布鍵を入力する入力ステップと、前記第２の暗号鍵に対応する固有の第２の復号鍵を用いて前記暗号化配布鍵を復号する処理および前記暗号化ディジタル情報を出力する処理の少なくとも一方を行うステップとを有することを特徴とする。

【００１９】

【作用】請求項１の発明では、配布するディジタル情報には固有に第１の暗号鍵・第１の復号鍵を割当て、各情報端末には固有に公開鍵暗号方式による第２の暗号鍵・第２の復号鍵を固有に割当てる。なお、第１の暗号鍵・第１の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は２つの鍵は同一のものとなる。

【００２０】情報供給局では、ディジタル情報は固有の第１の暗号鍵で暗号化して暗号化ディジタル情報を生成し、これを受信情報端末へ配布するとともに、受信情報端末が暗号化ディジタル情報を復号する際に必要な第１の復号鍵を上記したような受信端末固有の第２の暗号鍵で暗号化した暗号化配布鍵を配送する。

【００２１】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布するとともに、情報供給局から得た当該情報端末用に暗号化された暗号化配布鍵を他の情報端末用に暗号化しなおして伝える。

【００２２】受信端末は、暗号化された第１の復号鍵を該端末に固有の第２の復号鍵で復号して該第１の復号鍵を取出した後、この第１の復号鍵を用いて暗号化されたディジタル情報を復号する。

【００２３】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得える一方、該暗号化ディジタル情報の暗号化に用いた第１の暗号鍵に対応する第１の復号鍵を自端末に固有の第２の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【００２４】従って、著作権を保護しつつ、ディジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも２次的に配布することが可能である。

【００２５】また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。すなわち、本発明では、個々の情報端末ごとに固有に割当てられた暗号鍵が内蔵されている。このため、ある端末が破られて内蔵されていた暗号鍵が外部に知られたとしても、特定の端末の複製品だけが複数存在する状況になる。従って、破られた特定の端末向けに配布した情報に対しては正当に課金されないが、それ以外の情報に対する課金は正常に機能する。さらに、そのような状態では破られた鍵が特定された場合にその鍵を使用不能にする必要があるが、破られた鍵から端末が特定でき、その端末の鍵を更新するだけでよい。これに対し、従来のようにすべての情報端末に同一の暗号鍵が内蔵されている場合には全端末の暗号鍵を更新する必要が生じるが、それは極めて困難である。

【００２６】また、例えば請求項２の発明のように情報端末内に課金管理を行う装置を内蔵し、その装置により利用状態を管理すれば、配布情報の切り出しや複写などの編集行為に対しても課金を正常に行うことができる。

【００２７】また、請求項４の発明では、配布するディジタル情報には固有に第１の暗号鍵・第１の復号鍵を割当て、各情報端末には固有に第２の暗号鍵・第２の復号鍵を固有に割当てる。なお、第１の暗号鍵・第１の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は２つの鍵は同一のものとなる。また、第２の暗号鍵・第２の復号鍵は、慣用暗号方式による場合は同一のものとなる。

【００２８】情報供給局では、ディジタル情報は固有の第１の暗号鍵で暗号化して暗号化ディジタル情報を生成し、これを受信情報端末へ配布するとともに、受信情報端末が暗号化ディジタル情報を復号する際に必要な第１の復号鍵を上記したような受信端末固有の第２の暗号鍵で暗号化した暗号化配布鍵を配送する。

【００２９】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布する。この場合、請求項１の発明と異なる点は、他の情報端末に対して、必ず、情報供給局から受信情報端末用の暗号化配布鍵を配送する点である。

【００３０】受信端末は、暗号化された第１の復号鍵を該端末に固有の第２の復号鍵で復号して該第１の復号鍵を取出した後、この第１の復号鍵を用いて暗号化されたディジタル情報を復号する。

【００３１】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得える一方、該暗号化ディジタル情報の暗号化に用いた第１の暗号鍵に対応する第１の復号鍵を自端末に固有の第２の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【００３２】従って、著作権を保護しつつ、ディジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも２次的に配布することが可能である。

【００３３】また、請求項１の発明と同様に、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【００３４】また、例えば請求項５の発明のように情報端末内に課金管理を行う装置を内蔵し、その装置により利用状態を管理するために、配布情報の切り出しや複写などの編集行為に対しても課金を正常に行うことができる。

【００３５】また、本発明によれば、配布された情報を復号するためには情報供給局にアクセスする必要があり、そのアクセス行為を記録することにより情報供給局で課金管理をすることが可能となる。

【００３６】一方、請求項７の発明では、配布されるディジタル情報には固有に第１の暗号鍵・第１の復号鍵が割当てられ、情報端末には固有に公開鍵暗号方式による第２の暗号鍵・第２の復号鍵が固有に割当てられる。なお、第１の暗号鍵・第１の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は２つの鍵は同一のものとなる。

【００３７】情報端末には、ディジタル情報は固有の第１の暗号鍵で暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を復号する際に必要な第１の復号鍵を上記したような当該端末固有の第２の暗号鍵で暗号化した暗号化配布鍵が配布される。

【００３８】また、この情報端末は、既に暗号化ディジタル情報の配布を受けている場合、他の情報端末へ、当

該暗号化ディジタル情報をそのまま配布するとともに、既に獲得してある当該情報端末用に暗号化された暗号化配布鍵を他の情報端末用に暗号化しなおして伝えることができる。

【００３９】情報端末は、暗号化された第１の復号鍵を該端末に固有の第２の復号鍵で復号して該第１の復号鍵を取出した後、この第１の復号鍵を用いて暗号化されたディジタル情報を復号することができる。

【００４０】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得える一方、該暗号化ディジタル情報の暗号化に用いた第１の暗号鍵に対応する第１の復号鍵を自端末に固有の第２の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【００４１】従って、著作権を保護しつつ、情報端末は、ディジタル情報の配布を受けることができるばかりでなく、既に配布を受けている場合、他の情報端末へも当該ディジタル情報を２次的に配布することが可能である。

【００４２】また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【００４３】また、請求項８の発明では、配布されるディジタル情報には固有に第１の暗号鍵・第１の復号鍵が割当てられ、各情報端末には固有に第２の暗号鍵・第２の復号鍵が固有に割当てられる。なお、第１の暗号鍵・第１の復号鍵は、公開鍵暗号方式および慣用暗号方式のいずれを利用しても良く、慣用暗号方式による場合は２つの鍵は同一のものとなる。また、第２の暗号鍵・第２の復号鍵は、慣用暗号方式による場合は同一のものとなる。

【００４４】情報端末には、ディジタル情報は固有の第１の暗号鍵で暗号化した暗号化ディジタル情報と、この暗号化ディジタル情報を復号する際に必要な第１の復号鍵を上記したような当該端末固有の第２の暗号鍵で暗号化した暗号化配布鍵が配布される。

【００４５】また、既に暗号化ディジタル情報の配布を受けた情報端末から他の情報端末へは、暗号化ディジタル情報をそのまま配布することができる。受信端末は、暗号化された第１の復号鍵を該端末に固有の第２の復号鍵で復号して該第１の復号鍵を取出した後、この第１の復号鍵を用いて暗号化されたディジタル情報を復号する。

【００４６】ここで、本発明では、暗号化ディジタル情報を基本的には制限なく配布し得える一方、該暗号化ディジタル情報の暗号化に用いた第１の暗号鍵に対応する第１の復号鍵を自端末に固有の第２の暗号鍵で暗号化した暗号化配布鍵を獲得した情報端末のみが、暗号化ディジタル情報を復号することが可能である。

【００４７】従って、著作権を保護しつつ、情報端末は、ディジタル情報の配布を受けることができるばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも２次的に配布することが可能である。

【００４８】また、請求項１の発明と同様に、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその情報端末以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【００４９】

【実施例】以下、図面を参照しながら本発明の実施例を説明する。図１には、本発明の一実施例に係る情報配布システムの構成を示す。この情報配布システムは、利用者に情報を無償で配布し、情報の利用時に初めて課金を行うような情報配布形態を実現しようとする場合に好適であり、情報配布サービスを提供する情報供給局１０１、情報の伝達に供される通信システム（情報伝達媒体）１０２、情報の配布を受けるとともに、受けた情報をそのままあるいは加工して２次的に配布することができる情報端末１０３、および後述するように本システムで用いられる暗号鍵の管理などをするサービスセンタ１０４からなる。

【００５０】本実施例で扱う配布情報は、ディジタル化されたテキスト・音声・画像あるいはこれらが混在した形式であり、例えば、新聞、雑誌などの出版物に代表される文書（および静止画）情報や、音楽、映画などの視聴覚的な情報を含むものとする。

【００５１】情報供給局１０１は、情報端末１０３の要求等に応じて、有料の情報（特に著作物）の配布を行う。当該情報配布システム内に設ける情報供給局１０１の数は任意である。

【００５２】情報端末１０３は、情報供給局１０１から情報の配布を受ける機能、配布された情報を表示する機能の他に、情報を編集するための機能、他の情報端末との通信機能などを有する。そして、必要に応じ、受け取った情報をそのままあるいは加工して他の情報端末１０３に渡すことができる。情報端末１０３の数は任意である。

【００５３】サービスセンタ１０４は、個々の情報端末１０３の暗号鍵のデータベースを管理しており、必要に応じて情報供給局１０１もしくは情報端末１０３からアクセスされる。

【００５４】各局１０１，１０３，１０４間での情報の伝達は通信システム１０２を介して行われる。なお、ディジタル化された有料情報の配布や後述する必要な復号鍵等の伝達にはどのような形態のメディアを利用しても良く、通常の通信回線の他に、放送や記録媒体（例えばＣＤ－ＲＯＭやフロッピーディスク、メモリカードなど）を利用することも可能である。また、例えば有料情報と必要な復号鍵とで互いに異なる情報伝達媒体を利用

するように構成することも可能である。本実施例では、通信システム１０２として、通常の通信回線を利用することとする。

【００５５】本実施例では、通信回線等における配布途上データの不正取得や改ざんの保護を実現するために、有料情報は暗号化された状態で配布する。情報供給局１０１は、配布情報ごとに異なる暗号鍵および復号鍵（以下、配布鍵と呼ぶ）の組（ただし、暗号鍵と復号鍵が同一の場合もある）を設定し、配布情報を暗号鍵で暗号化しておく。情報端末１０３は復号機能を実装しており、配布鍵を取得すれば暗号化された配布情報を復号することができる。

【００５６】また、本実施例では、ディジタル情報の特徴を生かした利用形態をユーザに提供するために、情報のコピーは自由（無料）とし、表示や視聴などの行為を有料とする。また、配布された有料情報の全部または一部を編集する行為（例えば情報の一部を切り出し他のデータと合成するような行為；以下、情報の２次使用と呼ぶ）は禁止せずに認めることとし、その代りに情報の２次使用に対して課金をする。

【００５７】ここで、情報の配布自体に課金する代りに情報の利用行為に対して課金を行うためには、情報の利用を判別しその結果に応じて課金する機構が必要となる。まず、課金機構を実現する方法としては、例えば次の２つの方法が考えられる。

【００５８】１つの方法は、情報供給局１０１が配布鍵を特定の情報端末１０３向けに配布する行為を監視し、この行為の記録を取るものである。他の方法は、各情報端末１０４夫々に、情報の復号行為、情報の編集行為を検出する機構およびユーザの情報利用量を制御する機構（以下、課金モジュールと呼ぶ）を装備するものである。

【００５９】前者の方法は、情報供給局１０１からの有料情報の配布行為に対しては課金が行えるが、それ以外の行為（例えば情報端末１０３同士での有料情報の配布や情報の２次使用）は課金できないのに対し、後者の方法は、情報の配布自体を無料とし、情報を利用した時点で課金することができる。

【００６０】本実施例では、情報利用行為自体に対して課金を行うことのできる後者の方法を用いる。なお、後者の方法は、課金モジュールが正常に動作する限りにおいては情報利用量を制御できるが、そのためには課金モジュール自体を攻撃から守る必要があるとともに、加えて著作物単位の使用量を情報提供側が把握するために、課金モジュール内の利用記録を回収する手段が必要となる。これらの点に関し、本実施例では、“超流通システム”にて示されている課金モジュールの構成と利用記録の回収法を適用することができる。簡単に説明すると、次のような仕組みである。ユーザが有料情報を利用するたびに減額される利用可能度数情報（プリペイドカードに記録されているデータやクレジットに相当する）が存在し、これがユーザからは操作不可能な媒体（例えばＩＣカード）に記録されている。媒体内の利用可能度数情報が不足すると課金モジュールの制御により、配布情報の復号などが実行できなくなる。ユーザがその媒体を情報提供側（本実施例では情報供給局１０１）に返送すれば、情報提供側が利用可能度数を増やしてこれを再びユーザに配送する。この媒体内に著作物単位の利用記録を課金モジュールの操作により書き込むことにより、情報提供側で度数情報の更新とともに利用記録を回収できる。また、通信回線により利用記録を送信することもできる。通信回線による形態では、情報提供側から受け取り信号を受信しない限りは課金モジュールの制御により情報の利用が不可能となるように構成する。

【００６１】次に、以上説明した機能を実現する情報端末１０３の構成例を図２を参照しながら説明する。図２に示すように、情報端末１０３は、課金モジュール２０１、ユーザメモリ２０２、表示部２０３、コマンド入力部２０４、２次記憶インタフェース部２０５、利用度数記憶媒体インタフェース部２０６、通信部２０７を備えている。

【００６２】このうち課金モジュール２０１は、物理的に保護されたモジュールであり、その内部には図３に示すように実行制御部３０１、暗号器／復号器３０２、鍵記憶部３０３、課金管理部３０４、保護メモリ３０５が設けられている。課金モジュールを物理的に保護する方法には様々なレベルが存在するが、幾つか例を挙げると、モジュール全体を１チップＬＳＩにより構成する方法、入出力線以外のモジュール全体を樹脂で封止する方法、モジュールに物理的な不正アクセス検出機構を設ける方法、さらに不正アクセスを検出した場合にはモジュール内のメモリ内容等を消去するなどの方法がある。なお、物理的な不正アクセスとは入出力線以外の部分を直接プロービングする行為を想定しており、その具体的な検出機構は例えば、文献 Ryoichi Mori, Masaji Kawahara: “Superdistribution: The Concept and the Architecture”, Trans. of IEICE, Vol. E73, No. 7, pp. 1133-1146 に述べられている。

【００６３】課金モジュール２０１は、暗号化された情報を復号する機能、復号した情報を暗号化する機能、および復号した情報を編集するための機能を有し、情報の利用（復号・表示や編集）に対して課金をするとともに、課金できないときは情報の利用を禁止する制御を行う。なお、基本的には、復号された配布情報（平文）は課金モジュール２０１内部の保護メモリ３０５に保持され、外部から直接読み出すことはできない。ただし、後述するように、情報の２次利用がされる場合は、課金した後に復号された配布情報（平文）の一部を当該課金モジュール２０１の外部に出力する。

【００６４】ユーザメモリ２０２は、暗号化された情報

等を格納するためのものである。コマンド入力部２０４は、ユーザからのコマンドを受け付けるためのものであり、入力装置としては例えばキーボードおよび／またはいわゆるマウス等を利用することができる。情報端末１０３で用いられるコマンドには、配布情報の復号表示、（情報供給局１０１への）配布情報の要求、（他端末１０３への）情報の送信、（他端末１０３からの）情報の受信、情報の編集（２次使用）などが用意される。

【００６５】表示部２０３は、復号された配布情報等を画面表示したり、各コマンドに対応した画面、例えば編集画面や通信画面を表示したりする。利用度数記憶媒体インタフェース部２０６は、利用度数を記録するための利用度数記憶媒体２０８を収容するインタフェースである。利用度数記憶媒体２０８には、例えばＩＣカードを用いると好ましく、この場合、利用度数記憶媒体インタフェース部２０６には、ＩＣカードリーダを用いることができる。

【００６６】通信部２０７は、配布情報等の送受信を外部と行うための通信インタフェースである。すなわち、各情報端末１０３は、この通信部２０７を介して通信システム１０２に接続されている。

【００６７】２次記憶インタフェース部２０５は、配布された情報を記憶するための２次記憶（図示せず）を収容するインタフェースである。２次記憶には、情報を大量に記憶できるハードディスクやフロッピーディスクなどを用いると好ましい。

【００６８】以下、上記構成における動作例を概略的に説明する。前述したように配布された有料情報は暗号化されている。情報端末１０３では、配布情報の復号表示コマンドを受け付けると、情報の復号を行う前に、まず課金モジュール２０１内の課金管理部３０４が利用度数記憶媒体２０８内の残高度数を調べる。残高度数が復号表示に必要な度数以上であれば、実行制御部３０１に“実行可能信号”を送る。これを受けて実行制御部３０１は２次記憶（図示せず）もしくはユーザメモリ２０２から配布情報を課金モジュール２０１内の保護メモリ３０５に転送する。

【００６９】なお、配布情報が大量の場合には、実際に表示される領域の周辺だけを転送するようにしても良い。例えば、雑誌などの情報であれば表示部２０３で表示可能な頁サイズのデータだけを転送し、ユーザからの頁めくりコマンドの入力の度に対応するデータを転送するようにすると、処理が高速化できるので効果的である。

【００７０】実行制御部３０１は、課金モジュール２０１内の情報を鍵記憶部３０３に格納されている復号鍵を用い暗号器／復号器３０２の暗号機能により復号し、保護メモリ３０５に格納する。表示部２０３では保護メモリ３０５の内容にアクセスし、画面表示などを行う。

【００７１】課金モジュール２０１では、課金管理部３０４にて、例えば復号表示した頁数をカウントし、その都度、頁あたりの表示分の度数を度数記憶媒体２０８内の度数情報から減額する。度数記憶媒体２０８が外されている場合など、減額に成功しないときには課金モジュール２０１内の実行制御モジュール３０１が保護メモリ３０５の内容をクリアするなどの処理を行って、配布情報が利用できないようにする。

【００７２】ここで、情報端末１０３では情報の２次使用を行うことができる。この情報の２次使用としては、表示されている情報に対する切り抜き行為が典型的である。この場合、例えば範囲指定／ファイルへの保存をユーザコマンドとして実行することになる。そして、課金モジュール２０１は範囲指定コマンドからその領域の切り抜きに対する課金額を計算し、度数情報を参照し、減額可能であれば実行し、そうでない場合にはエラーメッセージを表示して実行しないようにする。課金額の計算に必要な料金情報は、配布物ごとに添付されており、“頁あたりの表示料金”、頁あたりの切り抜き料金”などのデータを含んでいる。

【００７３】なお、配布物について２次使用を許可／禁止することを示す情報を付加し、この情報に従って、２次使用を許可／禁止するように構成することも可能である。２次使用が禁止されている場合、復号された配布情報（平文）が課金モジュール２０１の外部へ出力されることはない。

【００７４】以上が、情報端末１０３の構成および機能である。次に、上述した構成を有する情報配布システムにおいて用いる情報配布（１次配布および２次配布）の方式を２種類のものについて説明する。

【００７５】図４は第１の情報配布方式を示しており、情報の配送に慣用暗号方式を、配布鍵の転送に公開鍵暗号方式を利用した構成である。各情報端末１０３の課金モジュール２０１内部の鍵記憶部３０３には、それぞれ固有の秘密鍵（復号鍵）が記憶されている。一方、公開鍵（暗号鍵）は情報供給局１０１および各情報端末１０３からアクセス可能な状態で公開されている。以下、本方式の説明では、情報供給局１０１から情報の配布を受けようとする情報端末＃ｉの秘密鍵をＳＫ＿ｉとし、公開鍵をＰＫ＿ｉとする。

【００７６】公開鍵の管理は、図１のサービスセンタ１０４内に公開データベースを設置することで行っても良いし、あるいは、公開鍵と情報端末＃ｉのＩＤ情報とを組にして織り込んだデータにサービスセンタ１０４がディジタル署名を行った“公開鍵証明書”を情報端末＃ｉが保有し、要求の都度公開鍵証明書を交換することで行ってもよい。

【００７７】情報供給局１０１では、情報Ｐごとに固有の“配布鍵ＷＫ＿Ｐ”を定め、情報を配布鍵により暗号化する。このときの暗号方式には、処理速度が高速な慣用暗号を利用する。この暗号化配布情報を、Ｃ＿Ｐ＝Ｗ

Ｋ＿Ｐ（Ｐ）と記述することにする。情報端末＃ｉは、配布鍵ＷＫ＿Ｐを得ることにより、暗号化配布情報を基にして通常の配布情報を復元することが可能である。

【００７８】以下、図５のフローチャートを参照しながら、情報供給局１０１から情報端末＃ｉへの情報の１次配布の手順を説明する。なお、情報供給局１０１では、既に、情報Ｐを固有の配布鍵ＷＫ＿Ｐで暗号化し、暗号化配布情報Ｃ＿Ｐおよび配布鍵ＷＫ＿Ｐをリンクして図示しない記憶装置に格納してあるものとする。

【００７９】最初に情報端末＃ｉから情報供給局１０１へ情報Ｐの配布の要求が発生する（ステップＳ１）。情報供給局１０１は要求元の情報端末＃ｉに対応する公開鍵ＰＫ＿ｉをサービスセンタ１０４から取得する（ステップＳ２）。

【００８０】情報供給局１０１と情報端末＃ｉの間で認証プロトコルを実行し、情報供給局１０１は情報端末＃ｉの正当性を確認する（ステップＳ３）。ここでの認証プロトコルは、相手端末が秘密鍵ＳＫ＿ｉを所持している事実を確認するものであり、例えば検査側（ここでは情報供給局１０１）から乱数を送り、被認証側（ここでは情報端末＃ｉ）がその乱数を秘密鍵ＳＫ＿ｉで暗号化して返送し、検査側では公開鍵ＰＫ＿ｉで逆変換して送信した乱数が現れることを検査すればよい。

【００８１】認証に成功した場合（ステップＳ４でＹｅｓの場合）、情報供給局１０１は、暗号化情報Ｃ＿Ｐに用いた配布鍵ＷＫ＿Ｐを記憶装置から検索し（ステップＳ６）、この配布鍵ＷＫ＿Ｐを情報端末＃ｉの公開鍵で暗号化する（ステップＳ７）。このようにして生成される情報を暗号化配布鍵と呼ぶことにするとともに、Ｄ＿ｉＰ＝ＰＫ＿ｉ（ＷＫ＿Ｐ）と表記することにする。

【００８２】次に、配布する情報Ｐの暗号化情報Ｃ＿Ｐを検索し（ステップＳ８）、暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｉＰを情報端末＃ｉに配布する（ステップＳ９）。

【００８３】上記１次配布により暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｉＰを受信した情報端末＃ｉは、課金モジュール２０１内の鍵記憶部３０３に格納してある秘密鍵ＳＫ＿ｉを用い暗号器／復号器３０２の復号機能により暗号化配布鍵Ｄ＿ｉＰから配布鍵ＷＫ＿Ｐを取り出し、さらに配布鍵ＷＫ＿Ｐで暗号化配布情報Ｃ＿Ｐを復号することができる。配布鍵ＷＫ＿Ｐは情報端末＃ｉの課金モジュール２０１外部には現れず、配布情報の保存時には、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｉＰがリンク付けされ格納される。

【００８４】なお、ステップＳ１で、情報端末＃ｉから情報供給局１０１へ情報Ｐの配布を要求することで情報配布を開始する代わりに、情報供給局１０１から情報端末＃ｉへ情報Ｐの配布を通知することで情報配布を開始することも可能である。

【００８５】次に、図６のフローチャートを参照しながら、情報端末＃ｉから情報端末＃ｊへの情報の２次配布の手順を説明する。なお、情報端末＃ｉは、既に、情報供給局１０１から配布情報Ｐに対応する暗号化配布情報Ｃ＿Ｐを入手しており、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｉＰをリンク付けし格納してあるものとする。

【００８６】情報供給局１０１からの１次配布の場合と同様に、最初に情報端末＃ｊから情報端末＃ｉへ情報Ｐの配布の要求が発生する（ステップＳ１１）。情報端末＃ｉは要求元の情報端末＃ｊに対応する公開鍵ＰＫ＿ｊをサービスセンタ１０４から取得する（ステップＳ１２）。

【００８７】次に、１次配布の場合と同様の方法で、情報端末＃ｉ、ｊの間で認証プロトコルを実行する（ステップＳ１３）。なお、このステップＳ１３の認証プロトコルの実行は省いても構わない。

【００８８】認証に成功した場合（ステップＳ１４でＹｅｓの場合）、情報端末＃ｉは暗号化配布鍵Ｄ＿ｉＰを検索する（ステップＳ１６）。次に、検索した暗号化配布鍵Ｄ＿ｉＰを基にして情報端末＃ｊに渡す暗号化配布鍵Ｄ＿ｊＰを生成する（ステップＳ１７）。まず、情報端末＃ｉは暗号化配布鍵Ｄ＿ｉＰと情報端末＃ｊの公開鍵ＰＫ＿ｊを課金モジュール２０１に入力する。課金モジュール２０１では、情報端末＃ｉ用の暗号化配布鍵Ｄ＿ｉＰから配布鍵ＷＫ＿Ｐを取り出し、さらに情報端末＃ｊに対応する公開鍵ＰＫ＿ｊで暗号化した情報端末＃ｊ用の暗号化配布鍵Ｄ＿ｊＰ＝ＰＫ＿ｊ（ＷＫ＿Ｐ）を生成する。

【００８９】次に、配布する情報Ｐの暗号化情報Ｃ＿Ｐを検索し（ステップＳ１８）、暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｊＰを、情報端末＃ｊに配布する（ステップＳ１９）。

【００９０】上記２次配布により暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｊＰを受信したを受信した情報端末＃ｊは、課金モジュール２０１内の鍵記憶部３０３に格納してある秘密鍵ＳＫ＿ｊを用い暗号器／復号器３０２の復号機能により暗号化配布鍵Ｄ＿ｊＰから配布鍵ＷＫ＿Ｐを取り出し、さらに配布鍵ＷＫ＿Ｐで暗号化配布情報Ｃ＿Ｐを復号することができる。配布鍵ＷＫ＿Ｐは情報端末＃ｊの課金モジュール２０１外部には現れず、配布情報の保存時には、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｊＰがリンク付けされ格納される。

【００９１】なお、ステップＳ１１で、情報端末＃ｊから情報端末＃ｉへ情報Ｐの配布を要求することで情報配布を開始する代わりに、情報端末＃ｉから情報端末＃ｊへ情報Ｐの配布を通知することで情報配布を開始することも可能である。

【００９２】本方式では、暗号化配布鍵Ｄ＿ｉＰからＤ＿ｊＰの作成のような暗号化配布鍵の変換処理は、２次配布の度に必要となるが、暗号化配布情報Ｃ＿Ｐ自体は

そのまま配布できる。通常、情報Ｐのサイズは配布鍵ＷＫ＿Ｐに比べ極めて大きいため、暗号化配布情報Ｃ＿Ｐを再暗号化することなく利用できるのは有効である。

【００９３】なお、公開鍵暗号としてＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号を用いた場合、同じＷＫ＿Ｐを複数の暗号鍵で暗号化することになるが、このような場合には攻撃法の存在が知られている。攻撃法の具体例は次の文献に詳しい。

・Ｊ．Ｈａｓｔａｄ，“Ｏｎ ｕｓｉｎｇ ＲＳＡ ｗｉｔｈ ｌｏｗ ｅｘｐｏｎｅｎｔ ｉｎ ａ ｐｕｂｌｉｃ ｋｅｙ ｎｅｔｗｏｒｋ”，Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ：Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ－ＣＲＹＰＴＯ’８５ ｐｒｏｃｅｅｄｉｎｇｓ，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ，ｐｐ．４０３－４０８．

そこで、公開鍵暗号としてＲＳＡ暗号を用いる場合は、ＲＳＡの１ブロックとして暗号化できる平文のサイズは慣用暗号による配布鍵のサイズよりも大きいため、例えば配布セッションごとに異なる乱数Ｒを生成し、Ｒ｜｜ＷＫ＿Ｐ（但し、｜｜はデータの連結を意味する）を暗号化配布鍵の平文として用いるなどすれば好ましい。

【００９４】次に、第２の情報配布方式について説明する。図７は、第２の情報配布方式を示しており、情報の配送および配布鍵の転送ともに、慣用暗号方式を利用した構成である。ただし、第１の情報配布方式のように、配布鍵の転送に公開鍵暗号方式を利用しても構わない。

【００９５】各情報端末１０３には、課金モジュール２０１内部の鍵記憶部３０３に固有の秘密鍵が記憶されている。この場合には、慣用暗号のため、秘密鍵は暗号化と復号化の両方に用いられる。以下、本方式の説明では、情報端末＃ｉの秘密鍵をＫ＿ｉとする。

【００９６】秘密鍵Ｋ＿ｉのデータベースはサービスセンタ１０４が管理しており、個々の情報端末１０３に対応する秘密鍵Ｋ＿ｉはサービスセンタ１０４のみが把握可能である。情報供給局１０１はサービスセンタ１０４にアクセスし、秘密鍵情報を取得できる。ただし、本実施例では、情報端末１０３からは秘密鍵情報を取得できないものとする。

【００９７】情報供給局１０１では、情報Ｐごとに固有の“配布鍵ＷＫ＿Ｐ”を定め、情報を配布鍵により暗号化する。このときの暗号方式には、処理速度が高速な慣用暗号を利用する。この暗号化情報を、Ｃ＿Ｐ＝ＷＫ＿Ｐ（Ｐ）と記述することにする。情報端末＃ｊは、配布鍵ＷＫ＿Ｐを得ることにより、暗号化配布情報を基にして通常の配布情報を復元することが可能である。

【００９８】以下、図８のフローチャートを参照しながら、情報供給局１０１から情報端末＃ｉへの情報の１次配布の手順を説明する。なお、情報供給局１０１では、既に、情報Ｐを固有の配布鍵ＷＫ＿Ｐで暗号化し、情報Ｐ、暗号化配布情報Ｃ＿Ｐおよび配布鍵ＷＫ＿Ｐをリンクして図示しない記憶装置に格納してあるものとする。

【００９９】最初に情報端末＃ｉから情報供給局１０１へ情報Ｐの配布の要求が発生する（ステップＳ２１）。情報供給局１０１は要求元の情報端末＃ｉに対応する公開鍵Ｋ＿ｉをサービスセンタ１０４から取得する（ステップＳ２２）。

【０１００】情報供給局１０１は情報端末＃ｉとの間で認証プロトコルを実行し、情報端末＃ｉの正当性を確認する（ステップＳ２３）。ここでの認証プロトコルは、相手端末が確かに秘密鍵Ｋ＿ｉを所持している事実を確認するものであり、例えば検査側（ここでは情報供給局１０１）から乱数を送り、被認証側（ここでは情報端末＃ｉ）がその乱数を秘密鍵Ｋ＿ｉで暗号化して返送し、検査側では端末＃ｉの鍵Ｋ＿ｉで逆変換して送信した乱数が現れることを検査すればよい。

【０１０１】認証に成功した場合（ステップＳ２４でＹｅｓの場合）、情報供給局１０１は、暗号化情報Ｃ＿Ｐに用いた配布鍵ＷＫ＿Ｐを記憶装置から検索し（ステップＳ２６）、この配布鍵ＷＫ＿Ｐを情報端末＃ｉの秘密鍵で暗号化する（ステップＳ２７）。このようにして生成される情報を暗号化配布鍵と呼ぶことにするとともに、Ｄ＿ｉＰ＝Ｋ＿ｉ（ＷＫ＿Ｐ）と表記することにする。

【０１０２】次に、配布する情報Ｐの暗号化情報Ｃ＿Ｐを検索し（ステップＳ２８）、暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｉＰを情報端末＃ｉに配布する（ステップＳ２９）。

【０１０３】上記１次配布により暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｉＰを受信した情報端末＃ｉは、課金モジュール２０１内の鍵記憶部３０３に格納してある秘密鍵Ｋ＿ｉを用い暗号器／復号器３０２の復号機能により暗号化配布鍵Ｄ＿ｉＰから配布鍵ＷＫ＿Ｐを取り出し、さらに配布鍵ＷＫ＿Ｐで暗号化配布情報Ｃ＿Ｐを復号する。配布鍵ＷＫ＿Ｐは情報端末＃ｉの課金モジュール２０１外部には現れず、配布情報の保存時には、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｉＰがリンク付けされ格納される。

【０１０４】なお、ステップＳ２１で、情報端末＃ｉから情報供給局１０１へ情報Ｐの配布を要求することで情報配布を開始する代わりに、情報供給局１０１から情報端末＃ｉへ情報Ｐの配布を通知することで情報配布を開始することも可能である。

【０１０５】次に、図９のフローチャートを参照しながら、情報端末＃ｉから情報端末＃ｊへの情報の２次配布の手順を説明する。なお、情報端末＃ｉは、既に、情報供給局１０１から配布情報Ｐに対応する暗号化配布情報Ｃ＿Ｐを入手しており、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｉＰをリンク付けし格納してあるものとする。

【０１０６】情報供給局１０１からの１次配布の場合と同様に、情報端末＃ｊから情報端末＃ｉへ情報Ｐの配布の要求が発生する（ステップＳ３１）。情報端末＃ｉは、情報Ｐの暗号化配布情報Ｃ＿Ｐを検索し（ステップＳ３２）、情報端末＃ｊへを送信する（ステップＳ３３）。なお、情報端末＃ｉから情報端末＃ｊに暗号化配布情報Ｃ＿Ｐを配布するにあたって、情報端末＃ｉは情報端末＃ｊとの間で認証プロトコルは実行しない。

【０１０７】次に、情報端末＃ｊは暗号化配布情報Ｃ＿Ｐの復号に必要な暗号化配布鍵Ｄ＿ｊＰを情報供給局１０１に要求する（ステップＳ３４）。情報供給局１０１はこの要求に応じてサービスセンタ１０４から情報端末＃ｊの秘密鍵Ｋ＿ｊを取得する（ステップＳ３５）。

【０１０８】次に、１次配布の場合と同様の方法で、情報供給局１０１は情報端末＃ｊとの間で認証プロトコルを実行し、情報端末＃ｊの正当性を確認する（ステップＳ３６）。なお、このステップＳ３６は、後述する情報供給局１０１から暗号化配布鍵を配布した時点で情報端末＃ｊに課金するような方法をとる場合は、暗号化配布鍵の配布先が確実に情報端末＃ｊであるかどうかを確認できるので有効である。また、後述する情報の利用時に初めて課金するような方法をとる場合は、この認証プロトコルの実行は省いても構わない。

【０１０９】認証に成功した場合（ステップＳ３７でＹｅｓの場合）、情報供給局１０１は、暗号化情報Ｃ＿Ｐに用いた配布鍵ＷＫ＿Ｐを検索し（ステップＳ３９）、この配布鍵ＷＫ＿Ｐを情報端末＃ｊの秘密鍵で暗号化して暗号化配布鍵Ｄ＿ｊＰを生成する（ステップＳ４０）。なお、暗号化配布鍵はＤ＿ｊＰ＝Ｋ＿ｊ（ＷＫ＿Ｐ）と表記する。

【０１１０】次に、暗号化配布鍵Ｄ＿ｊＰを情報端末＃ｊに配布する（ステップＳ４１）。上記２次配布により暗号化配布情報Ｃ＿Ｐおよび暗号化配布鍵Ｄ＿ｊＰを受信した情報端末＃ｊは、課金モジュール２０１内の鍵記憶部３０３に格納してある秘密鍵Ｋ＿ｊを用い暗号器／復号器３０２の復号機能により暗号化配布鍵Ｄ＿ｊＰから配布鍵ＷＫ＿Ｐを取り出し、さらに配布鍵ＷＫ＿Ｐで暗号化配布情報Ｃ＿Ｐを復号することができる。配布鍵ＷＫ＿Ｐは情報端末＃ｊの課金モジュール２０１外部には現れず、配布情報の保存時には、暗号化配布情報Ｃ＿Ｐとその暗号化配布鍵Ｄ＿ｊＰはリンク付けされ格納される。

【０１１１】なお、ステップＳ３１で、情報端末＃ｊから情報端末＃ｉへ情報Ｐの配布を要求することで情報配布を開始する代わりに、情報端末＃ｉから情報端末＃ｊへ情報Ｐの配布を通知することで情報配布を開始することも可能である。

【０１１２】この方式では暗号化配布情報Ｃ＿Ｐだけが２次配布可能であるので、２次配布情報だけでは情報の利用ができないのが欠点であるが、大量の情報である暗号化配布情報Ｃ＿Ｐは２次配布できる。

【０１１３】なお、上記各情報配布方式では、２次配布において、配布する情報Ｐに対応する暗号化情報Ｃ＿Ｐは情報端末１０３のユーザメモリ２０２や図示しない２次記憶等に格納されており、情報端末１０３は、暗号化情報Ｃ＿Ｐを検索して（ステップＳ１８，Ｓ３２）、これを配布することとした（ステップＳ１９，Ｓ３２）。その代わりに、情報端末１０３自信が復号して得た平文を受信端末１０３の暗号鍵（公開鍵）で暗号化したものを暗号化配布情報として配布しても良い。

【０１１４】また、図５、６、８、９のフローチャートに示される手順は、適宜修正して実施することが可能である。以上のように、上述した情報配布方式により、任意の情報端末１０３は情報供給局１０１もしくは他の情報端末１０３から所望の情報を取得できる。

【０１１５】次に、各情報配布方式による情報配布システムにおいて、有料情報の取得（あるいは情報の視聴）および有料情報の２次使用に対してどのようにして課金すればよいかを説明する。

【０１１６】図４に示した第１の情報配布方式では、情報供給局１０１からの配布以外に情報端末１０３同士での配布が行なわれるため、統一的に課金するためには各情報端末１０３に内蔵されている課金モジュール２０１にて有料情報の復号行為をカウントし、有料情報の復号の度に課金する方法が良い。

【０１１７】さらにその拡張としては、最初に一度復号するときだけ課金され、同じ情報の２度目以降の復号に対しては課金しないようにすることも可能である。これは、例えば一度復号した暗号化配布情報のシリアル番号を課金モジュール２０１内にリストとして保存しておくことで実現できる。

【０１１８】なお、情報供給局１０１は課金には直接結び付かないが、情報配布の記録を残しておくことで、その記録を不正端末の発見等に利用することができる。一方、図７に示した第２の情報配布方式では、有料情報を視聴するためには必ず情報供給局１０１から暗号化配布鍵を得る必要があるため、この行為を情報供給局１０１で記録すれば、有料情報の供給行為に対する課金を行なえる。すなわち、一度配布された情報は何度復号して表示しても一定料金とするものである。

【０１１９】なお、情報端末１０３内蔵の課金モジュール２０１を利用すれば有料情報の復号の度に課金する行為も可能であり、情報供給局１０１では暗号化配布鍵の発行の記録は残すものの、情報の配布は無料とし、課金はすべて情報端末１０３内蔵の課金モジュール２０１に委ねることもできる。すなわち、暗号化配布鍵を受けとっても、それを利用しない限り課金しないこととする。

【０１２０】なお、有料情報の２次使用は、第１の情報配布方式および第２の情報配布方式のいずれの場合においても、課金モジュール２０１の処理によって行なう。

ここで、図４に示した第１の情報配布方式と図７に示した第２の情報配布方式では、各情報端末１０３には固有の秘密鍵が格納されており、しかもその秘密鍵の内容は情報端末１０３のユーザに対しても秘密にされている。ただし、ユーザ端末１０３内に課金管理を行うモジュールが存在するため、悪質なユーザによりそのモジュールが攻撃され秘密鍵が漏洩する可能性がある。図７の第２の情報配布方式のシステムにおいて仮に、情報端末＃ｘの秘密鍵Ｋ＿ｘが漏洩したものとしよう。このとき、その秘密鍵Ｋ＿ｘを用いることにより、情報端末＃ｘ用に配布された情報を盗視聴できる。しかしながら、他の情報端末用に配布された情報は、秘密鍵Ｋ＿ｘでは復号できないので、盗視聴することは不可能である。すなわち、本方式では、たとえ特定の情報端末の秘密鍵が漏洩したとしても、任意の情報を盗視聴できるわけではなく、被害がシステム全体に波及することはない。

【０１２１】また、情報供給局１０１に対して情報端末＃ｘを装って任意の情報の配布を受けることもできるが、このようにすると、情報供給局１０１に記録される配布のログと、実際の情報端末＃ｘから回収される利用記録のログから不正が発覚し、情報端末＃ｘから秘密鍵Ｋ＿ｘが漏洩したことが判明する。このような場合には、秘密鍵Ｋ＿ｘを使用不能とし、情報端末＃ｘの鍵Ｋ＿ｘを更新すればよい。

【０１２２】このように、情報端末１０３の鍵を個別化したことにより、システムの健全性が大きく向上する。この点に関しては、図４の第１の情報配布方式のシステムでも同様である。ただし、このシステムでは、２次配布は情報供給局１０１の介在なしに実行されるため、情報供給局１０１のログだけでは不十分である。２次配布が行なわれた場合、その事実を送信側の情報端末１０３と受信側の情報端末１０３の両方に記録するようにし、それらの利用記録を先に述べたような方法で回収することにすればその記録をたどることにより不正を確認できる。

【０１２３】その後の鍵の無効化と更新は、先のシステムの場合と同じである。ここで、上述した各情報配布方式では、情報の１次配布および２次配布に慣用暗号方式を用いたが、その代わりに公開暗号方式を用いても同様の効果が得られる。この場合、受信端末１０３が暗号化配布情報を復号する際に必要な復号鍵（秘密鍵）のみを配布鍵とし、情報供給局１０１は、これを受信端末１０３に固有の暗号鍵（公開鍵）で暗号化した情報を該受信端末１０３に送れば良い。

【０１２４】また、前述したように、各局１０１，１０３，１０４間での情報の伝達には、どのような形態のメディアを利用しても良く、本実施例で用いた通常の通信回線の他に、放送や記録媒体（例えばＣＤ－ＲＯＭやフロッピーディスク、メモリカードなど）を利用することも可能である。なお、この場合の各局の構成は明らかであるので、詳細な説明は省略する。また、本発明は上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【０１２５】

【発明の効果】本発明に係る情報配布システムによれば、各情報端末には固有に暗号鍵・復号鍵を固有に割当て、配布するディジタル情報には固有に暗号鍵・復号鍵を割当て、ディジタル情報は固有の暗号鍵で暗号化したものを配布し、これに必要な復号鍵を受信端末に固有の暗号鍵で暗号化して配送するので、著作権を保護しつつ、ディジタル情報の配布を情報供給局から行なうばかりでなく、既に情報供給局から配布を受けている情報端末からそうでない情報端末へも２次的に配布することが可能である。また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその端末装置以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【０１２６】また、配布された有料の情報の編集などの２次使用に対しても課金を行うことができる。一方、本発明に係る情報配布方法によれば、情報端末には固有に暗号鍵・復号鍵を固有が割当てられ、配布されるディジタル情報には固有に暗号鍵・復号鍵が割当てられ、ディジタル情報は固有の暗号鍵で暗号化したものを配布し、これに必要な復号鍵を受信端末に固有の暗号鍵で暗号化して配送するので、著作権を保護しつつ、情報端末では、ディジタル情報の配布を受けることができるばかりでなく、既に配布を受けている情報端末から他の情報端末へも該ディジタル情報を２次的に配布することが可能である。また、特定の情報端末の物理的安全性が保証されなくなった場合に被害がその端末装置以外に及ばず、その情報端末の特定や鍵の更新などの処理も簡単に実行できる。

【図面の簡単な説明】

【図１】本発明の一実施例に係る情報配布システムの概略構成を示す図

【図２】同実施例における情報端末の構成例を示す図

【図３】同実施例における課金モジュールの構成例を示す図

【図４】本発明の一実施例に係る第１の情報配布方式を説明するための図

【図５】同方式における１次配布手順のフローチャート

【図６】同方式における２次配布手順のフローチャート

【図７】本発明の一実施例に係る第２の情報配布方式を説明するための図

【図８】同方式における１次配布手順のフローチャート

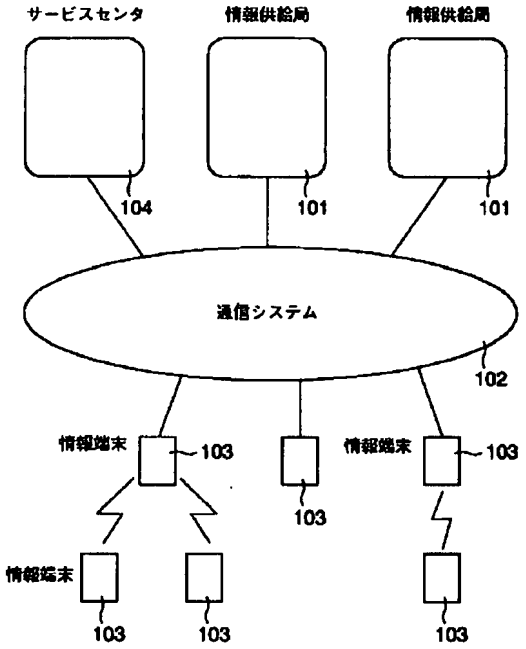
【図９】同方式における２次配布手順のフローチャート

【符号の説明】

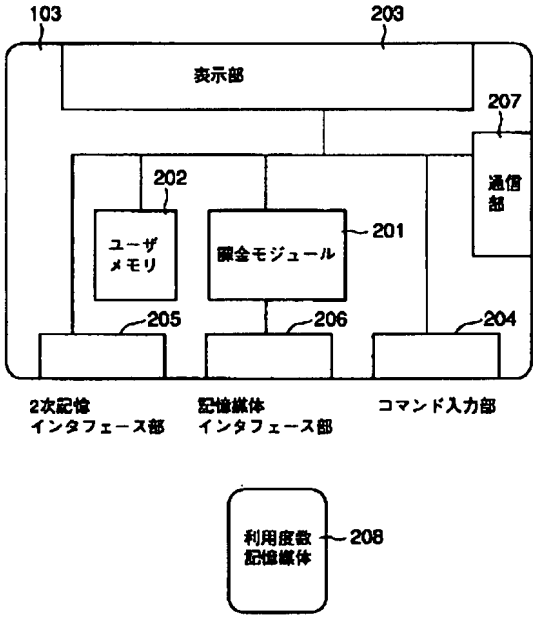
１０１…情報供給局、１０２…通信システム、１０３…情報端末、１０４…サービスセンタ、２０１…課金モジュール、２０２…ユーザメモリ、２０３…表示部、２０

４…コマンド入力部、２０５…２次記憶インタフェース部、２０６…度数記憶媒体インタフェース部、２０７…通信部、２０８…利用度数記憶媒体、３０１…実行制御部、３０２…暗号器／復号器、３０３…鍵記憶部、３０４…課金管理部、３０５…保護メモリ

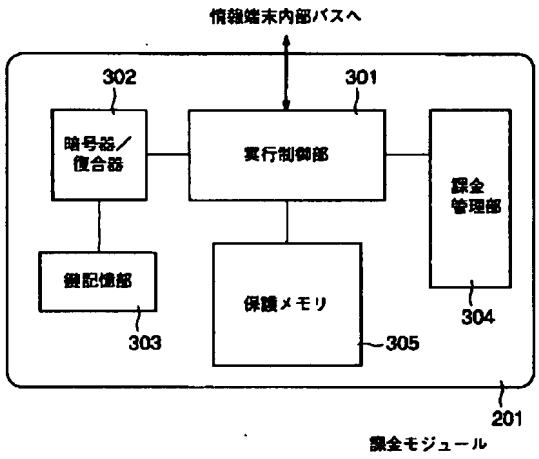
【図１】



【図２】

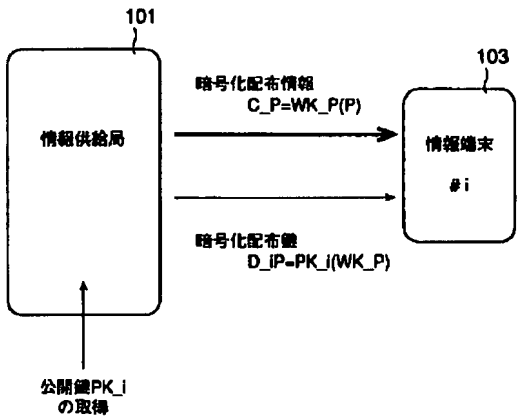


【図３】

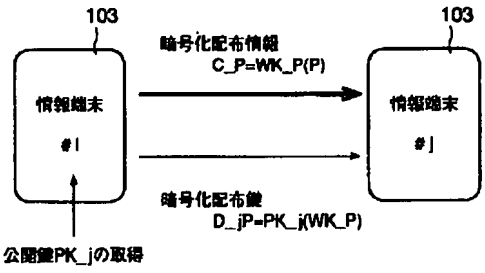


【図４】

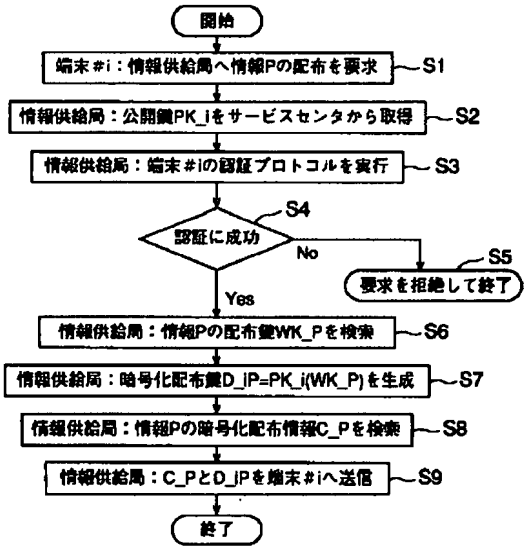
(a)



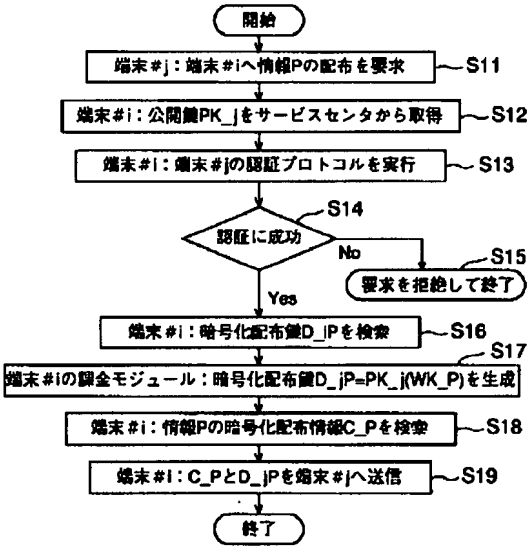
(b)



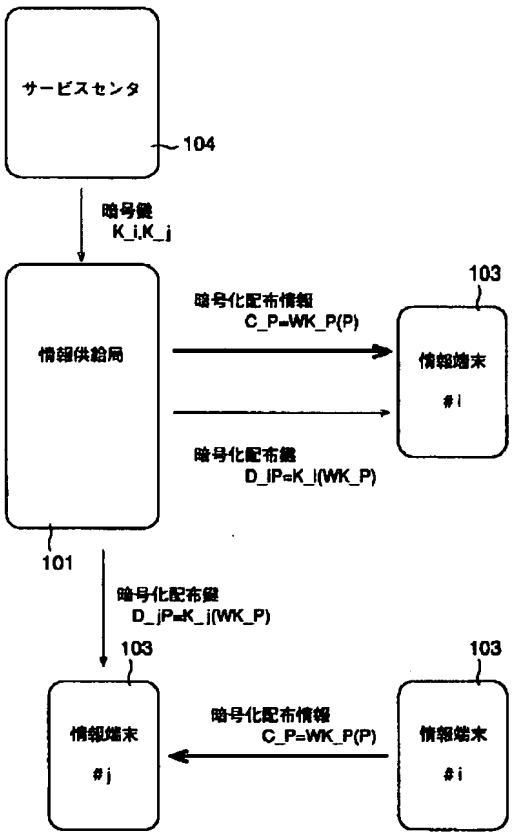
【図5】


開始
端末#i：情報供給局へ情報Pの配布を要求
S1
情報供給局：公開鍵PK_jをサービスセンタから取得
S2
情報供給局：端末#iの認証プロトコルを実行
S3
S4
認証に成功
No
S5
要求を拒絶して終了
Yes
情報供給局：情報Pの配布鍵WK_Pを検索
S6
情報供給局：暗号化配布鍵D_iP=PK_i(WK_P)を生成
S7
情報供給局：情報Pの暗号化配布情報C_Pを検索
S8
情報供給局：C_PとD_iPを端末#iへ送信
S9
終了

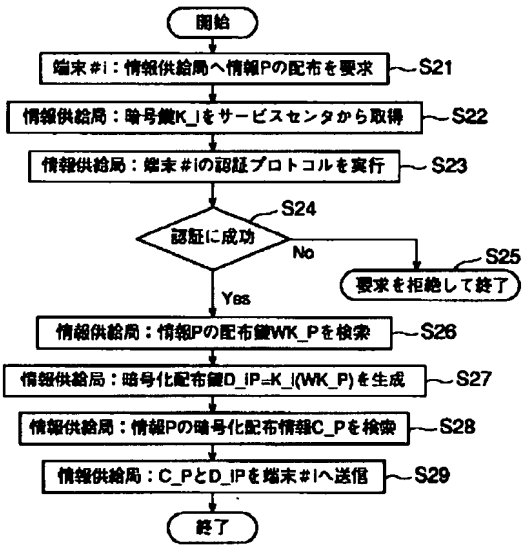
【図6】


開始
端末#j：端末#iへ情報Pの配布を要求
S11
端末#i：公開鍵PK_jをサービスセンタから取得
S12
端末#i：端末#jの認証プロトコルを実行
S13
S14
認証に成功
No
S15
要求を拒絶して終了
Yes
端末#i：暗号化配布鍵D_iPを検索
S16
S17
端末#iの課金モジュール：暗号化配布鍵D_jP=PK_j(WK_P)を生成
端末#i：情報Pの暗号化配布情報C_Pを検索
S18
端末#i：C_PとD_jPを端末#jへ送信
S19
終了

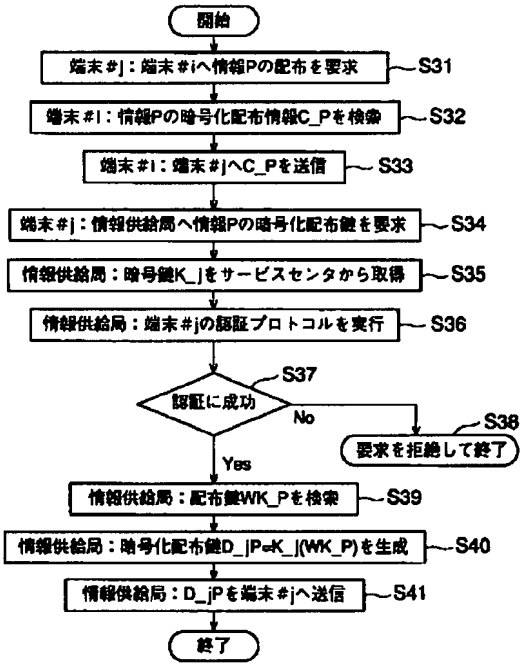
【図7】


サービスセンタ
104
暗号鍵
K_i,K_j
情報供給局
101
暗号化配布情報
C_P=WK_P(P)
暗号化配布鍵
D_iP=K_i(WK_P)
103
情報端末
#i
暗号化配布鍵
D_jP=K_j(WK_P)
103
情報端末
#j
暗号化配布情報
C_P=WK_P(P)
103
情報端末
#i

【図8】


開始
端末#i：情報供給局へ情報Pの配布を要求
S21
情報供給局：暗号鍵K_jをサービスセンタから取得
S22
情報供給局：端末#iの認証プロトコルを実行
S23
S24
認証に成功
No
S25
要求を拒絶して終了
Yes
情報供給局：情報Pの配布鍵WK_Pを検索
S26
情報供給局：暗号化配布鍵D_iP=K_i(WK_P)を生成
S27
情報供給局：情報Pの暗号化配布情報C_Pを検索
S28
情報供給局：C_PとD_iPを端末#iへ送信
S29
終了

【図９】


開始
端末#j：端末#iへ情報Pの配布を要求
S31
端末#i：情報Pの暗号化配布情報C_Pを検索
S32
端末#i：端末#jへC_Pを送信
S33
端末#j：情報供給局へ情報Pの暗号化配布鍵を要求
S34
情報供給局：暗号鍵K_jをサービスセンタから取得
S35
情報供給局：端末#jの認証プロトコルを実行
S36
S37
認証に成功
No
S38
要求を拒絶して終了
Yes
情報供給局：配布鍵WK_Pを検索
S39
情報供給局：暗号化配布鍵D_jP=K_j(WK_P)を生成
S40
情報供給局：D_jPを端末#jへ送信
S41
終了